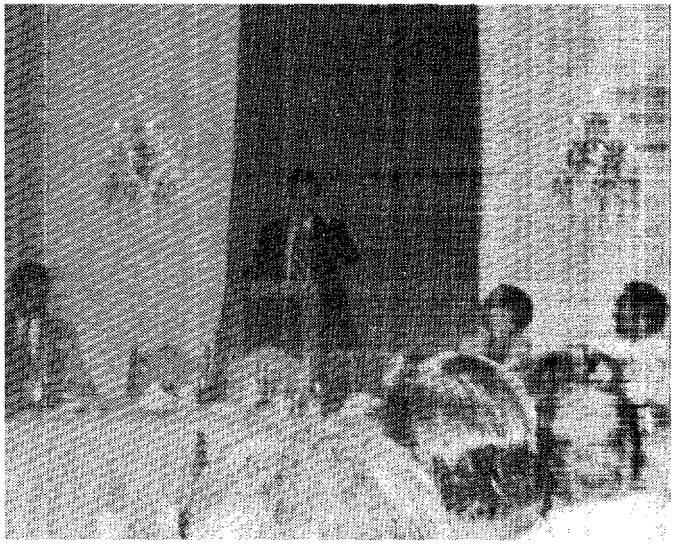
a f i REPORT

VOLUME 8 SEPTEMBER 1976 NUMBER 3



CIA DIRECTOR GEORGE BUSH SPEAKS AT LUNCHEON

Mr. George H. Bush, Director of the Central Intelligence Agency, was guest speaker at the Quarterly AFI Luncheon held at the Ft. McNair Officer's Club on September 10, 1976. Mr. Bush pointed out that there were popular misconceptions about his agency with its "James Bond image." He said that actually on any given day at lunch there is gathered in the Agency cafeteria persons holding the highest academic degrees given in many varied disciplines and that the CIA could staff a major university with the academic talent its staff possesses.

Mr. Bush acknowledged that he had become Director at the peak of the Congressional inquiry into certain operations of the CIA. He said that in less than nine months on the job, he had made at least thirty-five official appearances before Congressional committees. While he welcomes Congressional oversight, he indicated that a consolidation of the number of committees (now totaling seven) would be a major step in relieving the Director of the burden of repetitious appearances before Congress. Mr. Bush also commented that contrary to another popular misconception, every cent in the CIA budget is known to Congress.

Mr. Bush concluded his remarks by pointing out that under the law creating the CIA, the Director is obligated to keep the President informed on all matters involving the Nation's security, internationally. In order to carry out effectively this mission, the CIA must protect sources and methods of collecting and evaluating intelligence, he said. "We've got to have secrecy," he concluded and stated his full support of the concept of protecting identities of persons engaged in the Agency's various operations.

AFI TENTH ANNUAL AWARDS TO BE PRESENTED IN WASHINGTON ON OCTOBER 7

Six persons who have made substantial contributions to the investigative and enforcement field will receive the AFI annual awards on the evening of October 7, 1976, at a dinner at Ft. Myer's Officer Club outside Washington, D.C. Awards will be presented to the following in the categories named:

Judiciary	**Judge John J. Sirica** U.S. District Court
Legislative	**Cong. Peter W. Rodino, Jr. (D-NJ)**
Public Service	**Dr. Frances O. Kelsey** Food and Drug Administration
Law Enforcement	**Stuart H. Knight** Director, U.S. Secret Service
Legal	**Judge Harold R. Tyler, Jr.** Deputy Attorney General
Investigator of the Year	**Gerd Kaluski** San Francisco Chapter

Some who have received awards in past years:

The Honorable George L. Hart, Jr., U.S. District Court (Judiciary); **The Honorable John G. Tower**, U.S. Senate (Legislative); **Jerry N. Jenson**, Deputy Admin., Drug Enforcement Admin. (Enforcement); **Howard K. Smith**, American Broadcasting Company (Public Service); **The Honorable Luke C. Moore**, Superior Court, D.C. Government (Judiciary); **The Honorable Howard H. Baker**, U.S. Senate (Legislative); **The Honorable Clarence M. Kelley**, Director, FBI (Enforcement); **Marian Fox Burros**, Food Editor, The Washington Post and NBC (Public Service); **The Honorable Eugene T. Rossides**, Asst. Secy. for Enforcement, Treasury (Enforcement); **Mr. Jack Webb**, Mark VII, Universal City, CA, (Public Service); **The Honorable Roman L. Hruska**, U.S. Senate (Legislative); **The Honorable George Edwards, Jr.**, (Judiciary); **The Honorable Whitney N. Seymour**, U.S. Attorney, New York (Legal); **The Honorable Dante B. Fascell**, U.S. House of Representatives (Legislative); **Jerry V. Wilson**, Chief, Metropolitan Police

IN THIS ISSUE

Department (Enforcement); **The FEDERAL TIMES** (Public Service); **LIFE MAGAZINE** (Public Service); **The Honorable Carl Albert**, U.S. House of Representative (Legislative); **John H. Finlator**, Drug Enforcement (Enforcement); **The Honorable Warren E. Burger** (Judiciary); **The Honorable Fred M. Vinson, Jr.** (Legal); **The Honorable Tom C. Clark** (Judiciary); **The Honorable John L. McClellan**, U.S. Senate (Legislative); **BROOKINGS INSTITUTE** (Educational)

The awards dinner allows you an opportunity to meet and socialize with prominent people in enforcement and investigations. In addition, to enjoy an evening of good food, drink, fellowship and entertainment. Call the National Office (202) 347-5500 to make your EARLY reservations for a good table.

1975 Awards Dinner

AFI ENDORSES ESTABLISHMENT OF INSPECTOR GENERAL AT HEW

In a letter dated June 10, 1976, to The Honorable Jack Brooks, Chairman, Government Operations Committee, U.S. House of Representatives, the Association endorsed and recommended enactment of HR-5302 that would establish an independent office of Inspector General in the Department of Health, Education and Welfare.

CONTEMPORARY ISSUES TO BE DISCUSSED AT AFI SEMINAR ON OCTOBER 5, 6, 7, 1976

Experts in their field will discuss vital issues to you, the investigator, at the Tenth Annual Seminar in October. Louis Williams, Program Director, announces his usual excellent line-up of subjects to be discussed and the instructors:

TERRORIST ACTIVITIES: *Lt. Frank Bolz, Jr.*, CO, Hostage Negotiating Team, NYC Police Department; *Brooks McClure*, International Security Advisor, USIA.

REVISION OF EXECUTIVE ORDERS: *William T. Cavaney*, Executive Secretary, Defense Privacy Board; *Robert J. Drummond, Jr.*, Director, Bu Personnel Investigations, USCSC; *Robert R. Belair*, President's Domestic Council; *David H. McCabe*, Dir., Office of Security, State Dept.

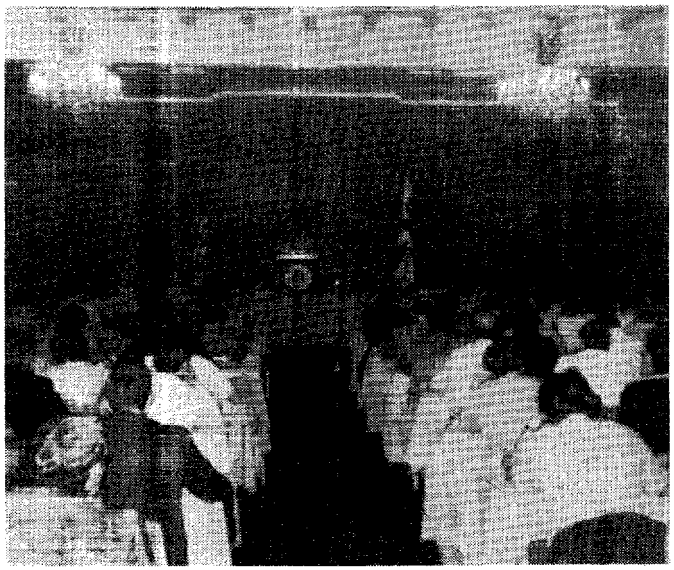
RECENT COURT DECISIONS: *August Bequai*, former Trial Attorney, Div. of Enforcement, SEC; *Eugene J. Kaplan*, former Spec. Asst. to Director, Criminal Investigations School, Treasury Dept.

NARCOTICS & THE [illegible] Training Institute, DEA: *Brian S. Boyd*, Office of Intelligence, DEA

FRAUD AGAINST THE GOVERNMENT: *James J. Graham*, Chief, Program Frauds, Criminal Division, Justice Department; *John Baber*, Unit Chief, Fraud & Bribery Units, White Collar Crime Section, FBI; *John J. Walsh*, Director, Office of Investigation, HEW.

PENDING LEGISLATION: *Timothy H. Ingram*, Staff Dir., House Sub-Com. on Government Info & Individual Rights; *Cathleen H. Douglas*, Attorney, Leva, Howes, Symington, Martin & Openheimer; *Hope Eastman*, Assoc. Director, American Civil Liberties Union.

Lou has combined an exceptional cross-section of talent representing both sides of the issues. Washington's magnificent October and excellent meeting facilities promises this Seminar to be one of the best for those in the investigative and security community. For more information, contact the National Office or Lou Williams at 202-653-6865.



1975 Seminar

COMPUTER CRIME: A SERIOUS DRAWBACK IN THE WAR AGAINST WHITE COLLAR CRIME

It is estimated that computer crimes cost the American public more than 100 million dollars yearly. Many say even this figure is a very conservative one. In a recent conference, I discussed the problem with a leading figure in law enforcement; he said, "Gus, we just don't know how to start. We're not trained for it." By "it" he meant technological crimes, especially computer frauds. Law enforcement officials are said to differ on many things. However, they tend to agree on one thing: neither prosecutors nor investigators have the training for the new crime wave made possible by the electronic revolution of the last 20 years.

Several years ago, the vice president of a national credit card company, with the aid of two accomplices and his company's computer, stole more than half a million dollars from his firm . . . just before Christmas. Four officers of a large New York bank stole more than one million dollars from their firm simply by altering deposit memos before they were [illegible] Recently, the Wall Street

Journal announced that a ring of computer criminals had been bilking national firms for a number of years for millions of dollars. Experts estimate that for every computer fraud that finally comes to the surface, dozens go on unnoticed. Even in those cases that are uncovered, prosecution is rare. Sentencing, when that finally takes place, is more of a "slap on the wrist." The "Jimmy Connors case" (an alias employed by Scotland Yard) best illustrates this. Jimmy took his firm for about half a million dollars with the aid of its computer. When finally discovered, the company directors called him to a meeting. Jimmy promptly admitted his crime and went on to advise his superiors that it would not be in their best interest to bring him to prosecution. "What will the public think, and also your creditors," he asked. The outcome was that Jimmy was given a letter of recommendation and a bonus and was packed on his way to another company.

Why, ask many, is law enforcement paralyzed in the war against the "electronic criminal." There are many reasons: (1) lack of knowledge as regards computers themselves; there is a "mystique" that somehow or other only a small and select few have this knowledge and thus the many shy away; (2) prosecution is difficult, lengthy and time consuming, and may tie up the manpower and resources of a prosecutor in one case for many years, whereas those same resources might be employed in many cases and thus show a greater volume of indictments and convictions; after all, nobody wants a real "tough fight"; (3) neither prosecutors nor investigators are equipped nor trained in this area; and (4) even when convictions are finally obtained, courts tend to be "soft" on white collar criminals. As one United States Attorney recently told me, "after a tough battle the 'guy' goes free."

The key to understanding a computer operation is the dividing of the process into five stages. Once the mechanics are understood, then the perpetration of the fraud becomes easier to grasp. The prosecution and sentencing areas are out of the province of the investigator and will be left to other articles. The first key stage is the "input" of data into the computer. Computer operators translate the data into a language that the computer understands. The data is "fed" into the computer through punch cards, magnetic tape units, optical scanners, and remote terminals. The frauds we usually read about usually occur at this stage. False data is fed into the computer and the machine is then usually programmed to perform certain acts which the criminal instructs it to do. The second key stage is "programming." This involves supplying the computer with step-by-step instructions for the solution of various problems. Programs can be tampered with or even destroyed. A computer can also be programmed to destroy the "false data" once the scheme has hatched, thus leaving no trail behind for the investigator. The third stage is the "central processing unit" (CPU). This is the central nervous system of the computer – the brain. It retrieves the necessary data and instructs the computer - (as programmed) - to perform the appropriate functions. The CPU is open to "terrorist attacks" and can also be destroyed by criminals who want to clean their "prints." The fourth step is the "output." Data ia received from the CPU and translated into intelligible form at this step. Many theft of data cases involve this stage. The final stage is the "communication" of data back and forth between computers or users and the computer. Telephonic circuits are usually used in the transmission process. This stage is open to the various electronic forms of "telephonic penetration." Use of codes may cut down some of the criminal attacks, but insiders and well organized gangs usually find access to such codes.

Computer crimes themselves usually fall into any of the following five categories: (1) "financial crimes" - this is usually performed were the computer is used for financial processing including payroll and storage of financial data; here the criminal will usually manipulate the "input" and "Programming" stages; (2) "property crimes" - the criminal uses the computer to obtain property rather than money, as for example as where he obtains the secret code and orders various supplies from the company and has them delivered to an address; (3) "information thefts" - this involves the theft of valuable data or programs, as was the case in the Encylopedia Britannica case where several employees stole the company's most "valued customer list," valued at some three million dollars, and sold it to a competitor; (4) "vandalism" - this takes the form of an attack against the computer itself, as for example by a disgruntled employee; in one such case, an angry computer operator removed the labels from more than 1000 reels of tape making identification almost impossible and creating havoc for a short period of time; and (5) "sabotage" - this may come from either agents of a competitor and take the form of industrial sabotage; it may also come from foreign agents of an enemy power, or "terrorists" - domestic or foreign - who either aim at the total destruction of the computer or holding it for ransom.

Knowledge and training are key factors in the war against electronic bandits. The latter is usually in his twenties, well educated and highly sophisticated. He may be a middle or even higher level executive. In the Equity Funding case it involved the top corporate structure and had it not been for a disgruntled employee, the scheme might still have gone on to the present unnoticed. The computer criminal is a serious problem. He presents the "world to come." Our defenses are poor; our laws in many cases antiquated and unable to even deter present traditional criminals, let alone a "super-breed" of criminals. The electronic crime wave raises in fact a key issue: is our criminal justice system able to cope with it or do we need change? A growing minority seems to be saying that we need a new approach.

–August Bequai
Attorney, Washington, D.C.
Vice-Chm. FBA Com. of Criminal Law
AFI Member

CUSTOMS SERVICE ISSUES 1975 REPORT

"Update 75" is the title of the 52-page publication issued by Customs which summarized the agency's varied activities during Fiscal Year 1975. The 52-page publication reviews Customs activities and accomplishments in the areas of collection and protection of the revenue, interdiction of all forms of contraband, including narcotics, and the enforcement of Customs and related Federal laws. Also included in "Update 75" are section detailing Customs long and event-filled history, and its highly successful ongoing anti-narcotics smuggling program. The appendix furnishes a wide range of statistics covering all Customs service functions. For more information call Brian Lee at 202-964-5286.

Editor's note: Tidbits from a recent Customs Service News Release: Customs officers discovered a man from Fremont, California, walking rather gingerly as he approached them. No wonder, they discovered he had a .25 caliber pistol and ammunition hidden in his shoes. And another: Customs

officers arrested John Simonelli, of Pawtucket, Rhode Island, following an inspection which showed Simonelli had $1,000 in stolen securities stuffed into his undershorts.

LEGISLATIVE WATCH

HR 214, now called the "Bill of Rights Procedures Act," was unanimously reported to the House Judiciary Committee by its Sub-committee on Courts, Civil Liberties and the Administration of Justice. Favorable committee action is expected on the amended bill which was on the top of the agenda when the committee returned to the fall session. As amended, the bill now carries the following provisions of interest to investigators:

Mail covers – Requests for mail covers by federal investigators must be supported by affidavits and resulting authorizations must be written and renewed every thirty days. Mail covers will only be authorized for the investigation of a felony, mail fraud or the location of a fugitive. Upon the conclusion of the investigation, unless a court orders otherwise, the subject must be notified of the cover.

Financial records – In order to gain access to the records of a subject maintained by a financial institution, telephone company or credit card company, a federal investigator has three choices. He may obtain the consent of the subject; he may obtain and serve a subpoena on both the subject and the company or bank; or, he may gain access with a search warrant from a court. The subject must be notified of his right to challenge such a subpoena in court unless such notification would "seriously jeopardize the investigation."

Wiretap – The amended bill would extend wiretap laws to forbid the interception of non-verbal electronic communications such as computer data, telegraph or telex, unless a court order is obtained. (The bill also enjoins private companies from monitoring employees' telephone calls unless it provides advance notice and designates the phone instruments subject to such interceptions.)

On the subject of wiretapping, a bill jointly sponsored by the White House and Senator Kennedy, S-3197, has been introduced in the Senate. The bill would bring wire-tapping activity under judicial control by establishing a requirement that a warrant be obtained in each case. The bill expands the scope of investigative activity authorizing wiretapping to include not only law enforcement but the gathering of foreign intelligence as well. It also would provide that for certain limited national security purposes, the President may authorize a wire intercept without a warrant. It provides that American citizens engaged in certain activities may be treated as foreign agents and monitored in search of foreign intelligence information.

Current polygraph legislation (Bella Abzug's HR-13191) has gone to the Subcommittee on Constitutional and Civil Rights of the House Judiciary Committee where it is being studied and reviewed with a view of updating background data. The bill would forbid the use of polygraphs in private and public employment practices. No hearings are scheduled during this Congress. Any AFI member having information he believes germane to the evaluation of this bill, or other ideas to offer, should contact the National Office or the Executive Secretary. The National Executive Committee is in contact with responsible congressional staff officials regarding consideration of the bill.

LETTER TO THE EDITOR

MR. KELLEY'S QUAGMIRE – ONE INVESTIGATOR'S OPINION

The Director of the FBI now finds himself the focal point of yet another controversy in the intelligence/law enforcement community. This truly is an era when journalists and Congressmen and now even senior executive branch bureaucrats clamor over each new scintillating tid bit which has a potential to embarrass the FBI or the CIA. This post-Watergate morality would be easier to swallow were it not applied so selectively.

I feel confident that in the future the woods will yield an over abundance of self ordained journalistic and congressional investigators who will thoroughly rake through Mr. Kelley's past and through their heretofore established investigative procedures, such as innuendo and statement out of context, will try to somehow be successful in tacking a "de Sade" to the end of his name.

It is opprobrious that a double standard continues to be applied by the very people casting the stones. The papers are full of revelations about our elected officials engaging in everything from soliciting prostitutes to taking bribes. It's rare when Congress even slaps the hand of one of its own for such indiscretions and the press conveniently cloaks all of its illegal acts under the First Amendment. I find nothing in the language of the First Amendment nor in the Federalist papers (which outlined our forefathers intentions) that even remotely can be construed as giving Daniel Schorr the right to violate Title 18 of the U.S. Code. No action was taken to reprimand Rep. William Alexander for assaulting a police officer a couple of years ago, but the Congress used its purse string powers to see to it that the officer who had the audacity to apply the law evenly, was himself fired. And that well known Congressperson on Capitol Hill with the wide brim hats and equally wide mouth who used high paid legislative assistants to unclog her toilet in the middle of the night; the least she can do is refund the federal treasury the appropriate plumbers fee.

The pity of this latest round of hypocrisy will be if they are successful in forcing Mr. Kelley to leave his office. The FBI has come under a lot of flak in recent years, but through it all the quality of work from the agent in the field remains high. I've had the privilege of working with a number of their agents and can attest to their high level of professionalism and expertise. Much of the credit for this has to be given to men in the upper echelons, like Mr. Kelley, who are responsible for maintaining high standards.

I hope the Director perseveres through this tribulation. Now if only the Congress would redistribute some of its time and aid us in putting the handcuffs where they belong – on the criminal element posing a danger to the safety of our people.

Member - AFI

AN INITIAL COMMENT ON THE LAW ENFORCEMENT IMPACT OF THE NEW RECORD KEEPING POLICIES

In public administration we are living in what has been called a new era with respect to information practices. Recent legislation and federal rule-making have enunciated broadly conceived policies with respect to the interests of the public. In essence they call for record handling and data maintenance in [illegible] more careful of his pri-

vacy. These policies also include a newly conceived public right of access to government information. Implementing programs are clearly changing the behavior of the bureaucracy, but to what ultimate extent is not yet evident. There are still many issues unresolved, and litigation and additional legislation will be required before anything like a consistent policy system will emerge.

In law enforcement, where there has been some special emphasis and attention, the new policies appear more clearly developed than in other areas. Major federal laws now affecting the information practices of various law enforcement agencies include the Freedom of Information Act (FOIA) as amended, the Privacy Act of 1974, and the Omnibus Crime Control and Safe Streets Act of 1968 as amended by the Crime Control Act of 1973. In response to this last legislation, the Department of Justice has issued regulations affecting the maintenance of records by all local and state criminal justice agencies receiving LEAA support.

The general intent of the new policies is to enhance democratic values such as due process and participatory government, and to reduce the potential abuses of the purely administrative approach to law enforcement. Some initial concern has been expressed by law enforcement officials that these policies would somehow tip the balance too much in favor of the individual to the detriment of effective crime control and law enforcement. What effects may we really expect?

At the federal level, the FOIA establishes a "right" of public access to government information. But, it is carefully qualified with a number of specific exception. Investigative information that would reveal the identity of a *bona fide* confidential source or would compromise a criminal law enforcement investigation, may be withheld from subject individuals and the public. Unwarranted invasion of privacy is also excluded. Under the FOIA, some portions of federal investigative manuals and directives have been obtained by private individuals. However, other actions have been proposed that may be in the public interest. For example, the act may be used to discover the considerations underlying the exercise of prosecutorial discretion in certain federal cases and give the public a better insight into the functioning of federal investigative and regulatory agencies.

The Privacy Act provides that there may be no secret system of records on individuals, that an individual must be able to discover if he is a subject of a record, and that there may be no unforeseen use of such records. This requires that the identity, purposes and routine uses of such systems must be published along with instructions for individual access to them. However, even the existence of a record need not be revealed if it would alert the subject of a current investigation and compromise prosecution or fair adjudication. The Privacy Act has caused the disclosure through public notices that many non-investigative systems of personal records are routinely examined for law enforcement and other investigative purposes.

Under both the Privacy Act and the Department of Justice regulations, individuals must be given access to records pertaining to themselves and given the opportunity to request correction or amendment. (Again, records of on-going investigations are exempted.) The net effect of this provision may well be to make criminal record information more accurate in cases where the subject makes an inquiry.

The most extensive impacts on law enforcement are through the Department of Justice regulations which affect virtually all criminal justice agencies. They give the states until December 31, 1977, to establish procedures to assure [illegible] or executive orders for regulation of the dissemination of criminal record information to non-criminal justice agencies, and the dissemination of non-conviction data within the system. In the formulation of specific policies, considerable discretion has thus been handed to the states.

It is interesting to note how these regulations have been modified since their initial proposal in 1974. The final version omits earlier restrictions on the dissemination of conviction data and information regarding offenses for which a suspect is currently within the criminal justice system. It also removes earlier limitations on access to court records of public proceedings.

Another proposal now dropped from the regulations would have required special computer equipment dedicated to the processing of criminal history records. This expensive provision has been replaced with a more general requirement for personnel and physical security programs for the protection of such information.

A final provision that bears mention is the requirement that disposition information be included with arrest records before dissemination may be made under most circumstances. This, along with the LEAA policy of encouraging the establishment of centralized state repositories for criminal information, may serve to increase the accuracy and usefulness of the records. Consistent attention to the quality and timeliness of criminal history record information may cause the "new" policies to have an effect similar to that of the Miranda decision which was also viewed with some alarm at its inception. That effect was to ultimately contribute to more effective law enforcement processes.

Indeed, most of these information policies are not new. In one jurisdiction or another they have already been followed without adverse effect. At the federal level, in spite of the attention certain closed cases obtained under the FOIA have received in the press, there has been no evidence presented that current law enforcement investigations or prosecutions have been adversely affected. Of course, many law enforcement officials see a potential risk to certain sources and have testified to it, as last month's article on the Freedom of Information Act indicated.

How sweeping will be the eventual change in the law enforcement bureaucracy, only time will tell. One must conclude at this point that these policies portend nothing contrary to the public interest or effective law enforcement.

–Everett E. Mann
Adjunct Professor, Center for
the Admin. of Justice
The American University
AFI Member

"Every man
owes a part of his time and money
to the business or industry
in which he is engaged.
No man
has a moral right to withhold
his support from an organization
that is striving to improve
conditions within his sphere."

–President Theodore Roosevelt–1908

CODE OF ETHICS
ASSOCIATION OF FEDERAL INVESTIGATORS

Conduct all investigations within the framework of the United States Constitution and with due regard for individual rights regardless of race, creed or national origin.

Develop and report the facts of an investigation completely, accurately and objectively without fear or favor.

Demonstrate by work and deed in your professional and private life that a Professional Investigator is worthy of confidence and trust. Adhere to the highest moral principles in the pursuit of official duties as well as in the conduct of your private life.

Avoid, in the course of an investigation, any act or failure to act which could be considered to have been motivated by reason of personal or private gain.

Consider it a sacred trust to protect the source of information obtained in confidence.

Make a continuing effort to improve your professional knowledge and technical skill in the investigative field.

Assist other members of the Association in their official duties and professional advancement.

AVAILABLE TO MEMBERS

AFI Badges $9.00

AFI Decals . . . . . windshield 35¢
regular 50¢

Obtain from Chapter Treasurer or from National Office.

DON'T YOU HAVE SOMETHING TO SAY?

Items of general interest to investigators are encouraged and urgently needed by the editor. Do you have an article, an opinion, or a comment? Please keep in mind that we can continue to publish the AFI REPORT only if we have material to print. Take a few minutes of your time to help and let us hear from you.

Membership maintains a PROFESSIONAL ASSOCIATION. HAVE YOU PAID YOUR DUES?

AFI REPORT
Published by
Association of Federal Investigators
****

Address all communication to:
National Office, 815 - 15th Street, N.W.
Washington, D.C. 20005
Phone: 202-347-5500

Association of Federal Investigators
815 Fifteenth Street, N.W.
Washington, D.C. 20005

Non-profit Organ.
U.S. Postage
PAID
Permit No. 43154
Washington, D.C.

(CIA)
PUBLIC AFFAIRS OFFICER ML
CENTRAL INTELL. AGENCY
WASHINGTON, DC 20505

1 F 04

ORG1 Association of Federal Investigators
CIA.01 Bush, George

ASSOCIATION OF FEDERAL INVESTIGATORS

NATIONAL OFFICE • 815 FIFTEENTH STREET, N.W. • WASHINGTON, D. C. 20005

Area Code (202) 347-5500

QUARTERLY LUNCHEON

FRIDAY, SEPTEMBER 10, 1976

$5.00 Per Person

Cash Bar: 11:30 AM

Lunch: 12 Noon

****

SPEAKER: GEORGE BUSH
DIRECTOR
CENTRAL INTELLIGENCE AGENCY

+ AF attended

****

Place: Ft. McNair Officers' Club
P St. bet. 3rd & 4th, SW
Washington, D. C.

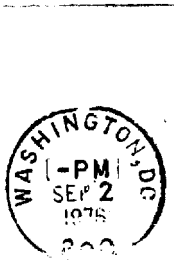
FREE PARKING

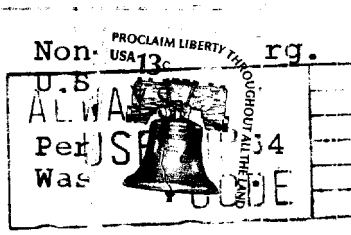
****

PLEASE CALL NATIONAL OFFICE, 347-5500 FOR RESERVATIONS

PLAN TO BE WITH US - CALL EARLY FOR RESERVATIONS FOR YOU AND YOUR GUESTS

Association of Federal Investigators
815 15th Street, NW
Washington, DC 20005





(CIA)
PUBLIC AFFAIRS OFFICER ML
CENTRAL INTELL. AGENCY
WASHINGTON, DC 20505

1F04

ORGI Association of Federal

ASSOCIATION OF FEDERAL INVESTIGATORS

NATIONAL OFFICE • 815 FIFTEENTH STREET, N.W. • WASHINGTON, D. C. 20005

Area Code (202) 347-5500

July 14, 1976

The Honorable George Bush
Director
Central Intelligence Agency
Washington, D. C. 20505

Dear Sir:

With pleasure we look forward to having you as our guest speaker at our luncheon to be held at Ft. McNair on Friday, September 10, 1976.

The speakers table will include leaders in the field of investigations and enforcement and we will be honored to have you with us at this time.

Please let me know if you have any questions or if I can be of any help to you.

Sincerely,

Louis T. Williams

Louis T. Williams
Executive Secretary

 ORG1 Association of Federal Investigators

DCI PUBLIC APPEARANCE

Event: Association of Federal Investigators Luncheon Speaker

Place: Ft. McNair, Washington, D. C.

Date: September 10th

Time: 12:30 p.m. -- Lunch begins

Speaking from Text — Yes ✓ — No ____

Need Press Office Help to Prepare Text "excerpts" — Yes ✓ — No ____

Hand Out Text ____

Limited Release ____

Embargoed Release ____

Want Press Office to Attend — Yes ✓ A.F. — No ____

Press Conference — Yes ____ — No ____

Need Press Office Help to Set Up Press Conference — Yes ____ — No ____

Special Press Assistance Required ____

Comments: Discuss: 2 weeks before for subject & help with excerpts.

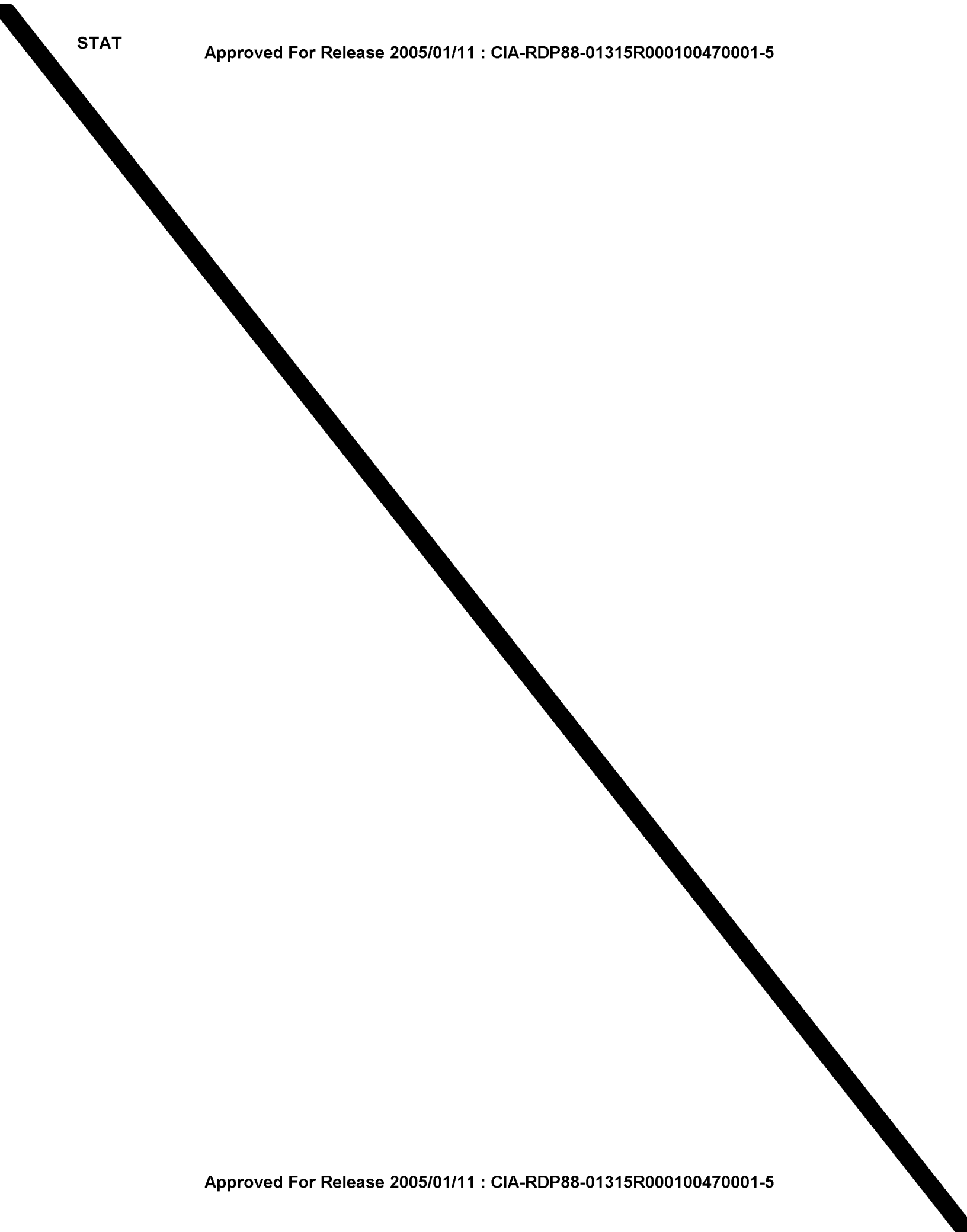
Travel Arrangements ____

Marvin Shelton will be at door 7-9-76 GLS

Contact: Mr. Terjensen -- 692-6987

Officers Club, Ft McNair

Arrive 12:15 P.M



Approved For Release 2005/01/11 : CIA-RDP88-01315R000100470001-5

WASHINGTON POST
2 Sept 1977

R. Kessler, Ron
CIA 3.01.7
Wallace, Clyde
Org Associations?
Federal Investigators

New Bug All Ears—Snoops Through Hung-Up Phone

By Ronald Kessler
Washington Post Staff Writer

A breakthrough in electronic listening devices permitting any home or office to be bugged and tapped without entering it was disclosed by a wiretap expert at a conference of federal law enforcement and security investigators here yesterday.

The device can be placed anywhere on a line leading to the phone to be tapped — on telephone poles, in underground cable vaults, or in telephone company switching offices miles away. It picks up both telephone calls and conversations in the room where the phone is installed, even when the receiver is on the hook.

This feature, said government bugging experts who were queried yesterday, would make it unique.

According to Clyde Wallace, a bugging equipment manufacturer who disclosed the development, the device is already being used by two federal investigative agencies.

Wallace described the device at a symposium of the Association of Federal Investigators at the Mayflower Hotel. Others on the three-day agenda were officials of the Justice Department, Federal Bureau of Investigation, Bureau of Narcotics and Dangerous Drugs, and Treasury Department.

Spokesmen for the FBI and Central Intelligence Agency declined yesterday to comment on whether their agencies were the ones alluded to by Wallace in his speech as using the device.

The FBI has primary responsibility for court-approved wiretapping, which is interception of telephone calls, and bugging, which is monitoring of room conversations through electronic devices. The CIA conducts extensive electronic surveillance outside the U.S. but is not supposed to operate domestically unless the matter is related directly to its foreign intelligence work.

After his speech, Wallace expressed surprise and some dismay that a reporter had been present while he talked. He declined to answer any questions on the new device.

During the speech, however, Wallace described it as the first method for simultaneously tapping a phone and bugging the room where it is installed without tampering with the phone or even going near the premises.

To tap and bug a phone, he said, the device is placed anywhere on the telephone line running to it. It then emits a radio frequency, which trips a switch in the phone. This switch normally prevents conversations in the room from traveling over the telephone wire. When it is bypassed by the signal, the phone becomes an open microphone, transmitting both room conversations and telephone calls to the listener.

Normal phone calls can be made while the device is in operation, according to Wallace, who said he is developing his own version of the device.

Last year, a cut-off switch was found by an electronics expert to be bypassed on the civil defense telephone in the office of Maryland Gov. Marvin Mandel, making the phone capable of transmitting conversations from Mandel's office. The telephone company attributed the situation to a wiring error.

Other devices, called infinity transmitters or "harmonica" bugs, can bug and tap phones simultaneously, but they all require physical entry to permit rewiring of the phone or installation of a bug.

Government bugging experts interviewed yesterday said no public mention had been made before of a device that would not require entry, and several expressed surprise at the development.

However, Bernard Fensterwald, former chief counsel of former Sen. Edward E. Long's Subcommittee on Administrative Practice and Procedure, which held extensive hearings on government surveillance, said he has had information for some time from nonpublic disclosures during the committee's investigation that security agencies, such as the CIA, use such a device.

Wallace earlier this year was investigated by the FBI to determine if any devices sold by the Spy Shop, which he owns, violate federal wiretap laws, according to FBI sources.

Wallace said he operates strictly within the confines of the law. The outcome of the FBI investigation could not be learned yesterday.

Asked about the propriety of an FBI official appearing on the same agenda with the target of an FBI probe, an FBI spokesman said the FBI representative appeared on a different day than did Wallace. Other than that, he said, the bureau would not comment.